Architecture des systèmes d'automatisation des postes résiliente aux attaques des trames GOOSE

Maëlle Kabir-Querrec, Stéphane Mocanu, Pascal Bellemain, Jean-Marc Thiriet, Eric Savary

Architecture des systèmes d'automatisation des postes résiliente aux attaques des trames GOOSE

M. Kabir-Querrec[1,2], S. Mocanu[1], P. Bellemain[1,] J.-M. Thiriet[1], E. Savary[2]
1) Univ. Grenoble Alpes, GIPSA-lab, F-38000 Grenoble, France
CNRS, GIPSA-lab, F-38000 Grenoble, France
2) Euro-System, F-38760 Varces, France

Résumé : Notre travail concerne la spécification et la mise en œuvre d'un système d'automatisation des postes électriques conformes à la norme IEC 61850 capable de fonctionner en présence d'attaques sur les systèmes de communication temps-réel (communication GOOSE). Notre architecture repose sur trois concepts : la réalisation des sondes capables de détecter les attaques sur les trames GOOSE, la remontée des alertes au SCADA et la réalisation d'une commande des équipements de terrain intégrant l'information de cybersécurité.

Mots clés : IEC 61850 ; Attaques GOOSE ; Protection électrique ; Architecture résiliente ; SCADA ; SAS.

I. Introduction

1. L'automatisme des postes IEC 61850

Les réseaux de distribution électrique modernes (smart-grids) intègrent des technologies intelligentes dont l'objectif est de régler en temps-réel la production de l'électricité ainsi que sa distribution afin d'optimiser le comportement global du système (satisfaction de la demande *versus* minimisation des pertes). Cette fonctionnalité de contrôle en continu du comportement du réseau est réalisée via l'automatisme du réseau de distribution qui implémente les fonctions classiques d'acquisition de données, supervision et commande (*Supervisory Control and Data Acquisition – SCADA*). Etant données la taille et la complexité du réseau électrique un contrôle centralisé n'est pas envisageable. L'intelligence du réseau repose sur des fonctions de contrôle distribuées. La brique de base de ce système de contrôle distribué est le *système d'automatisation de poste (Substation Automation System – SAS)*. Le standard IEC 61850 définit le poste comme étant "un ensemble d'équipements électriques interconnectés avec des fonctionnalités communes". Le système d'automatisation de poste est constitué de l'ensemble des équipements informatiques réalisant des fonctions de mesure, contrôle, protection électrique. Ces équipements sont appelés *Equipements Electroniques Intelligents (Intelligent Electronic Device – IED)*. La réalisation de certaines fonctions complexes dans les SAS, notamment des fonctions de protection électrique, nécessitent l'utilisation des informations fournies par des IED distincts (par exemple des mesures de courant en plusieurs points de réseau). Il s'ensuit que la réalisation des SAS nécessite un système de communication adéquat.

2. SAS et sûreté de fonctionnement

La définition d'un tel système de communication est l'un des objectifs de la norme IEC 61850. Les deux grands atouts de ce standard (première édition 2003) sont l'interopérabilité des systèmes de contrôle, qui met fin à la dépendance d'une infrastructure envers un unique fournisseur, et le passage de l'information par le réseau Ethernet qui permet d'éliminer quantité de câbles jusqu'alors nécessaires au transfert de l'information point à point. Afin de pouvoir déployer les technologies 61850 à l'ensemble du réseau électrique, il s'est révélé nécessaire d'apporter plus de fiabilité dans ce système d'automatisme basé sur les communications. C'est chose faite dans la seconde édition (2013) qui supporte l'Ethernet gigabit et qui est enrichie de méthodes de

redondance au niveau couche liaison : boucles PRP (Parallel Redundancy Protocol) et HSR (High-availability Seamless Redundancy). Ces mesures vont dans le sens de la fiabilité, de la disponibilité et plus globalement de la sûreté de fonctionnement. Ainsi, il est désormais concevable d'utiliser les technologies IEC 61850 dans des systèmes critiques tels qu'une centrale de production thermique ou nucléaire dans laquelle une perte ou une altération des communications impacterait la continuité de service mais pourrait aussi avoir des conséquences plus dramatiques.

Notre travail s'inscrit dans la continuité de ces mesures visant à assurer la sûreté de fonctionnement des systèmes IEC 61850 : il concerne l'étude d'une architecture résiliente à des attaques sur les communications en temps-réel dur, basée sur la détection d'intrusion. La détection d'intrusion est l'une des deux seules mesures de sécurité énoncées comme faisables pour le protocole GOOSE dans le standard IEC 62351 [IEC 2009], l'autre étant l'authentification par signature numérique, hors du scope de ce travail. Ce standard porte sur la sécurité des données et des communications dans les infrastructures électriques dont la sûreté de fonctionnement, la sécurité et la fiabilité reposent de plus en plus sur l'intégrité du système d'information et de communication.

3. Communication dans les postes : flux horizontaux et verticaux

La norme IEC 61850 spécifie plusieurs méthodes de communication selon les besoins temps-réel des différentes fonctions ainsi que les protocoles associés. Dans le contexte de cette étude deux méthodes seront utilisées : les communications locales, en temps-réel dur (4ms de délai de propagation application) et la communication avec le SCADA.

La figure 1 présente la disposition typique des flux de communication dans le SAS. La réalisation des fonctions nécessite une communication en temps-réel entre les IED. Cette communication est implémentée via des transmissions multicast de trames Ethernet (type 0x88b8 dites *GOOSE – Generic Object Oriented System Event*). La communication avec le SCADA est réalisée par TCP/IP avec un protocole application MMS (*Manufacturing Message Specification* - ISO 9506). Notons que, souvent, les flux "verticaux" et "horizontaux" circulent sur des réseaux physiquement différents (réseaux supervision et temps-réel séparés).

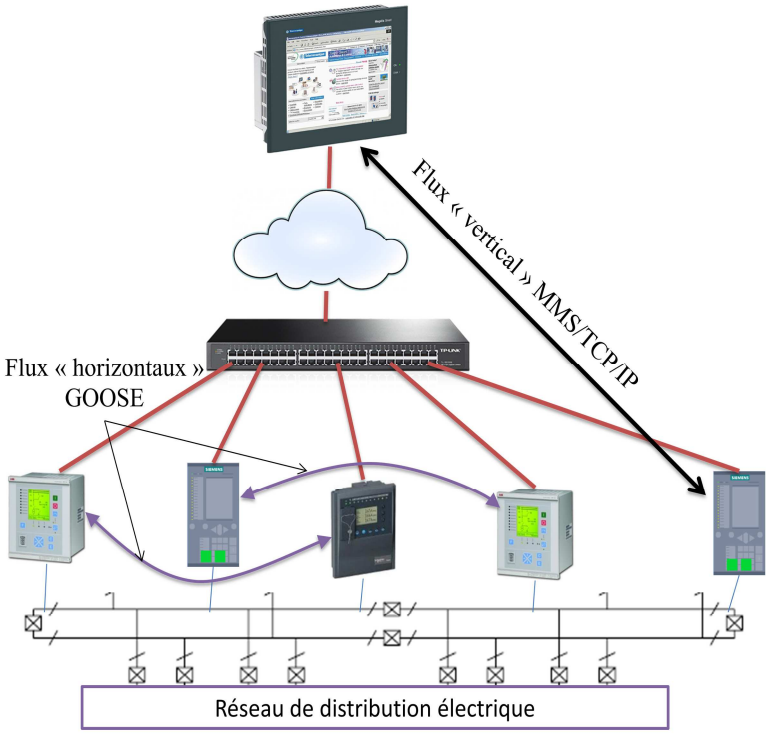

Figure 1. Flux de données 61850 : commuté "horizontal" (GOOSE) vs. "vertical" SCADA

II. Fonctionnement du protocole GOOSE

1. Structure d'une trame GOOSE

Le protocole GOOSE est mappé sur la couche liaison Ethernet. Les messages sont envoyés en broadcast selon un mécanisme d'éditeur – abonné (*publisher – subscriber*) : les appareils branchés sur le réseau voient l'ensemble des trames GOOSE mais n'interceptent que celles qui les intéressent, les messages GOOSE auxquels ils sont abonnés.

La structure de la trame GOOSE est standardisée (ISO/IEC 8802-3), elle est rappelée dans le standard IEC 61850 et a fait l'objet de plusieurs publications dont [Kriger 2013]. Elle est détaillée dans la figure 2. L'APDU (*Application Protocol Data Unit*) correspond aux données transmises par l'application émettrice. Il est spécifié en ASN.1 comme une séquence de 12 éléments (à droite sur la figure 2).

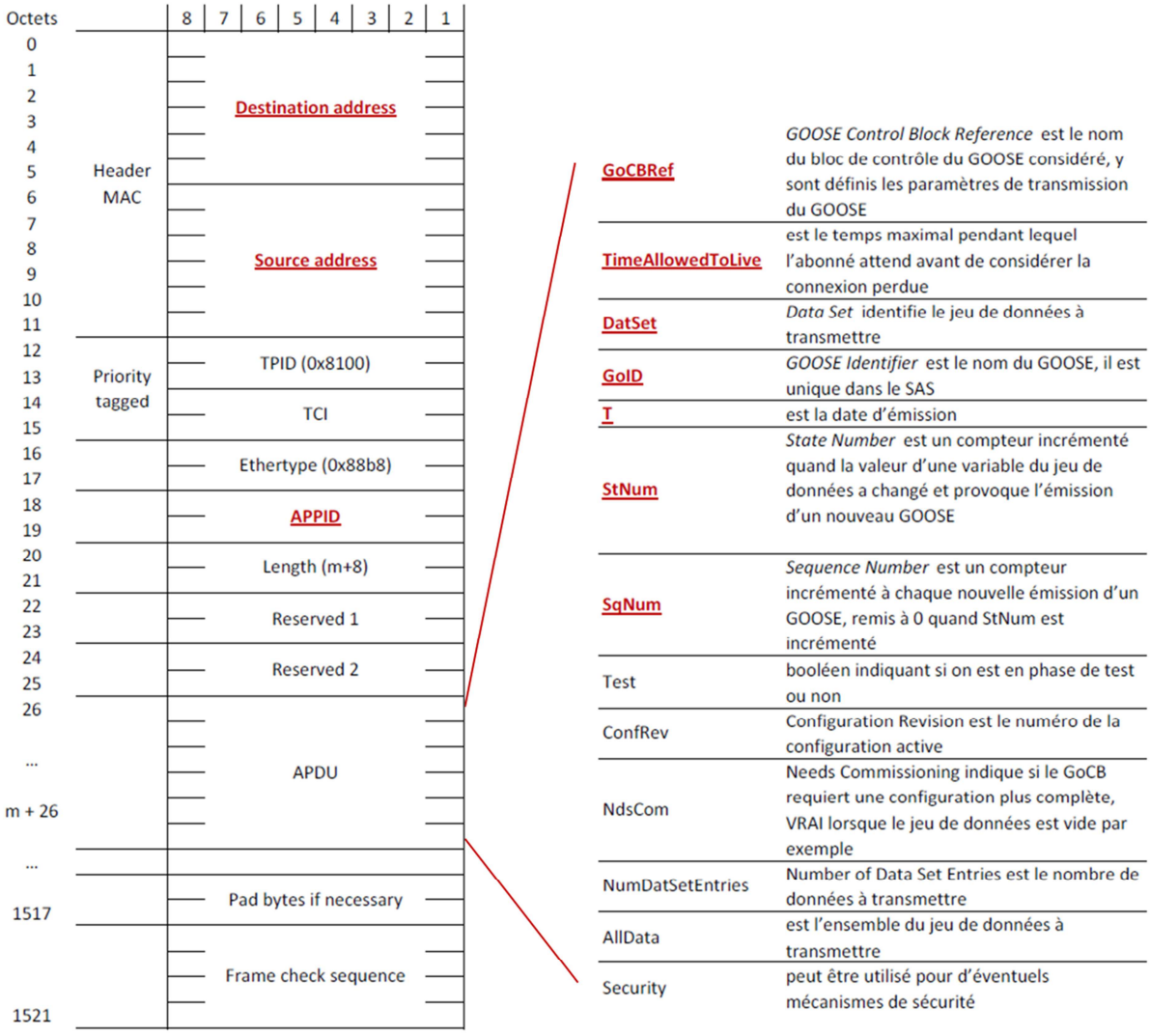

Figure 2. Structure d'une trame GOOSE (d'après IEC 61850-8.1)

Notons que le champ "Security" est prévu dans l'APDU de la trame GOOSE présenté dans la norme IEC 61850 mais son utilisation n'est pas explicitée. Les mécanismes de sécurité sont en fait recommandés dans le standard mais leur mise en œuvre est laissée à la discrétion des concepteurs d'IED.

Les champs dont le nom est souligné seront exploités dans ce travail pour vérifier la conformité du message avec la configuration du SAS.

2. Mécanisme de transmission du protocole GOOSE

Le mécanisme de transmission éditeur – abonné ne permet pas d'acquitter la réception du message. Pour assurer un certain niveau de fiabilité, le protocole GOOSE utilise un schéma particulier de retransmission comme illustré dans la figure 3. Lorsqu'un événement se produit, impliquant un changement de valeur de l'une ou plusieurs des données transmises par GOOSE, il déclenche l'envoi d'un message GOOSE en incrémentant StNum et en remettant à 0 SqNum. Cette trame GOOSE est retransmise à grande fréquence d'abord (T1) puis le rythme ralentit (T2, T3) jusqu'à atteindre la durée correspondant à des conditions stables. SqNum est incrémenté à chaque émission.

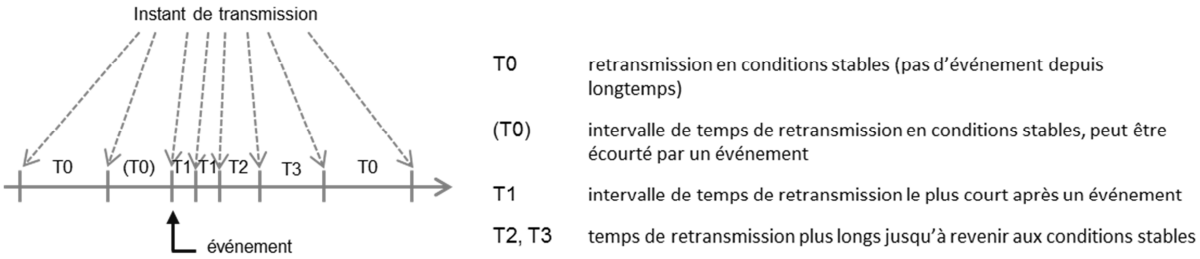

Figure 3. Schéma de transmission des messages GOOSE

III. Détection d'intrusion sur le réseau GOOSE

1. Description des attaques

Nous considérons deux types d'attaques sur les trames Ethernet, attaques déjà répertoriées dans la littérature. Le premier type d'incident considéré est la tempête Ethernet. Ce type d'incident a été, par exemple, à l'origine d'un arrêt d'urgence d'une centrale nucléaire aux Etats-Unis [NRC 2007]. Dans le cas d'un poste IEC 61850, la conséquence d'une tempête Ethernet sur le réseau dédié aux communications GOOSE serait un incident de type DoS (*Denial of Service*). Les trames GOOSE ne pourraient alors pas être réceptionnées par leurs abonnés dans le temps imparti de 4ms mettant en péril le bon déroulement des mécanismes de protection. Malgré la procédure de retransmission détaillée ci-dessus, il est probable qu'un IED ne reçoive pas plusieurs occurrences d'un message GOOSE d'affilée. Or chez certains fabricants, l'hypothèse est faite qu'au maximum une occurrence d'un message GOOSE est perdue et les IED sont paramétrés pour ignorer les trames dont les numéros de séquence et d'état ne respecteraient pas cette hypothèse [Siemens 2014]. La connexion entre l'émetteur et l'abonné est alors rapidement considérée comme perdue.

Le second type d'attaque est l'injection sur le réseau de messages GOOSE usurpés, faussement interprétés par les appareils abonnés comme valides. Comme cela a été montré dans [Hoyos 2012], une telle attaque peut être implémentée dès qu'un accès au réseau temps-réel GOOSE est assuré. Il est alors possible de déclencher des actions non souhaitées telles que basculement d'un switch, ouverture d'un disjoncteur, etc… ou d'envoyer des messages frauduleux de coordination à d'autres sous-stations.

2. Etat de l'art

La sécurisation des systèmes embarqués est une préoccupation grandissante dans la mesure où elle est garante de la sécurité des personnes et des infrastructures. Divers domaines sont concernés tels que l'automobile [Koopman 2013], l'aéronautique [Dessiatnikoff 2012], les usines chimiques et autres infrastructures critiques, etc... Comme souligné dans [Koopman 2013], une attaque de type spoofing (usurpation d'adresse source) permet à un attaquant de compromettre la sécurité d'un système embarqué et de ses usagers de multiples manières, quasi illimitées. Il suffit d'un accès au réseau Ethernet pour injecter des messages de contrôle aux actionneurs qui tiennent un rôle critique du point de vue sûreté de fonctionnement.

La sécurisation des réseaux de systèmes de contrôle et en particulier des SCADA passe en général par la détection de communications suspectes :

- soit au périmètre du système afin d'empêcher qu'elles ne pénètrent la zone à sécuriser (firewall) [Fovino 2012]. Le défaut principal de cette approche est de ne pas apporter de protection pour les attaques lancées depuis l'intérieur du réseau, ce qui est le cas par exemple des deux types d'attaques considérées dans cette étude.
- soit au sein même du système afin d'avertir les opérateurs et de déclencher des mesures défensives (*IDS* et *IPS – Intrusion Detection / Protection System*) [Cheung 2007], [Premaratne 2010], [Hong 2014]. Ces deux derniers articles traitent spécifiquement de la détection d'intrusion réseau pour les protocoles multicast IEC 61850 tels que GOOSE.

Le travail proposé ici ne consiste pas uniquement à identifier des communications suspectes. Il s'agit d'apporter une réponse avec un mode de fonctionnement dégradé tolérant à une situation d'insécurité cyber. C'est l'idée sur laquelle s'appuient également les travaux de [Kirsch 2014]. L'architecture de supervision est constituée de plusieurs réplications du SCADA, implémentées différemment les unes des autres, qui doivent collaborer pour traiter les informations reçues du poste et générer une commande acceptée par toutes les entités (redondance hétérogène). Ainsi, l'application peut continuer à fonctionner de façon fiable dans la mesure où le nombre d'instances du SCADA corrompues ne dépasse pas un certain seuil. Cependant cette approche s'applique pour des communications verticales SCADA – sous-station quand nous nous intéressons aux échanges horizontaux temps-réel internes à la sous-station pour lesquels une telle stratégie n'est pas envisageable (puissance et temps de calcul).

Une piste proposée dans [Koopman 2013] pour sécuriser les communications multicast temps-réel est de développer des fonctions d'intégrité et d'authentification, afin d'empêcher des attaques de type spoofing qui seraient détectées directement par les appareils destinataires des messages. C'est une idée intéressante. Toutefois, nous avons fait le choix dans ce travail de proposer une solution extérieure aux IED et qui, de plus, va un pas plus loin que la détection avec un mode de fonctionnement alternatif.

IV. Notre approche

Notre proposition d'architecture résiliente repose sur les principes suivants :

- des flux "verticaux" (échanges de données avec le SCADA) sûrs et sur un réseau distinct du réseau temps-réel [Kirsch 2014],
- l'existence des sondes capables de détecter les tempêtes Ethernet ainsi que les GOOSE usurpés ("IDS niveau Ethernet"),
- la remontée des alertes des IDS Ethernet vers le SCADA,
- la réécriture des programmes de commande des IED en prenant en compte les alertes des IDS envoyés via le SCADA.

La suite de l'article décrit notre solution aux trois derniers points ci-dessus.

1. Les "IDS Ethernet"

Nous avons modifié deux logiciels de monitoring du réseau afin d'obtenir les détecteurs des tempêtes Ethernet et des messages GOOSE usurpés.

A partir d'un moniteur de bande passante disponible en Linux (nous avons choisi ifstat, mais bmon, bmonNG, slurm, ntop on vnstat peuvent également être utilisés), nous avons créé une sonde de mesure de l'utilisation de bande passante instantanée et moyenne sur des durées configurables par l'utilisateur. Les données sont remontées au SCADA via un serveur de données utilisant un protocole industriel (dans la première version nous avons utilisé un serveur Modbus/TCP de par sa simplicité).

La détection des messages GOOSE usurpés est bien plus délicate. Tel qu'il a été présenté dans [Hoyos 2012] une attaque GOOSE envoie une séquence rapide de trames GOOSE (un faux changement d'état au niveau de l'émetteur) qui, dans le cas d'une attaque "parfaite", respecte les numéros de séquence et les horloges des trames légales. La figure 4 présente le chronogramme d'une telle attaque.

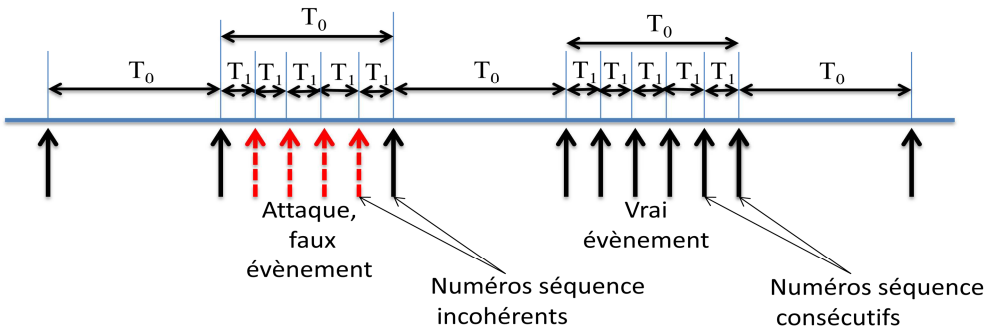

Figure 4. Vrais (traits pleins) et faux (pointillés) évènements dans les séquences de GOOSE

Une attaque GOOSE "imparfaite" peut être détectée en comparant les numéros des trames et horodatages de deux GOOSE successifs. Mais même dans l'hypothèse d'une attaque GOOSE parfaite, celle-ci sera détectée au plus tard après un temps T_0, le premier message GOOSE légal après ou pendant l'attaque mettant en évidence l'incohérence des numéros de séquence.

Notre détecteur de trames GOOSE usurpées est créé à partir de l'analyseur de trafic tcpdump.
Nous vérifions pour chaque trame GOOSE :

- que le message GOOSE reçu correspond à une connexion GOOSE définie dans le système en contrôlant les champs suivant : Source address, APPID, GoCBRef et GoID,
- la cohérence des compteurs StNum et SqNum par rapport au message GOOSE précédent ayant le même GoID (GOOSE Identifier),
- la cohérence de la date d'émission avec le message GOOSE précédent ayant le même GoID ainsi qu'avec les compteurs StNum et SqNum.

Afin de réduire le délai de propagation des alarmes vers le SCADA en cas de détection de faux messages GOOSE (messages fabriqués par un intrus), nous avons couplé notre sonde à un client Modbus/TCP, le superviseur étant configuré en serveur.

2. Intégration au SCADA

Les données des sondes remontées soit périodiquement (scrutation du serveur Modbus de la sonde mesurant la bande passante), soit spontanément (messages événementiels envoyés par le détecteur des messages GOOSE usurpés) sont exploitées au niveau du superviseur SCADA pour la prise de décision du basculement des équipements du système (IED) en mode dégradé/sécurité. L'architecture générale est présentée en figure 5.

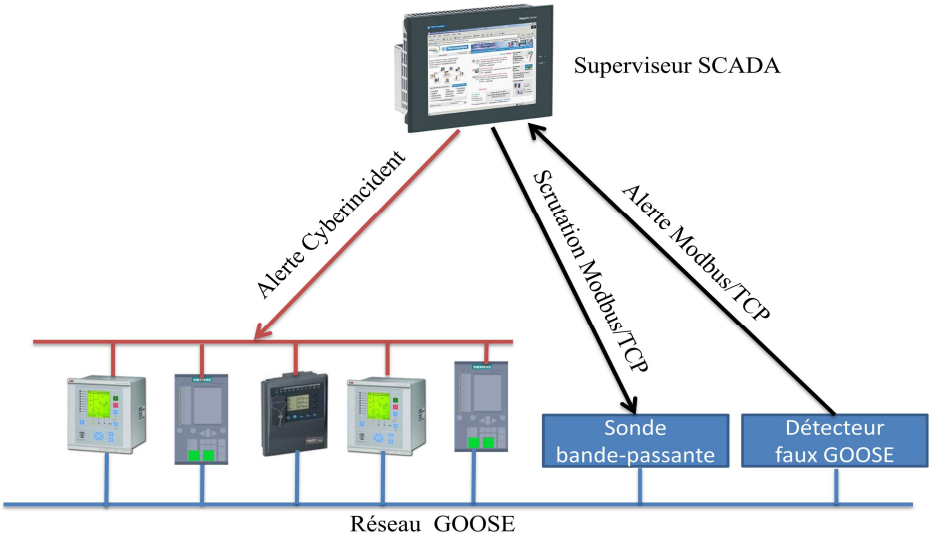

Figure 5. L'architecture de communication proposée

3. Programmation résiliente des IED

La dernière étape dans la réalisation de notre système résilient aux attaques est la prise en compte de l'alerte cyber-incident au niveau du programme de l'IED. Basculer d'un mode de fonctionnement à l'autre est simple au niveau de l'écriture des diagrammes de commande (voir figure 6). La difficulté réside dans la synthèse de la fonction "sûre".

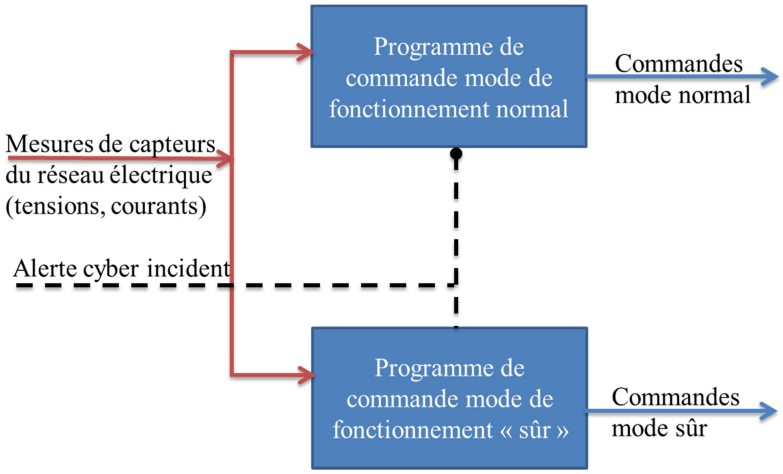

Figure 6. Basculement du mode de fonctionnement sûr / cyber-incident

3.1 Synthèse du mode de fonctionnement sûr : cas général

Nous proposons une méthode dérivée de l'AMDE (Analyse des Modes de Défaillance et leurs Effets), inspirée de la synthèse des modes de fonctionnement dégradés en cas de panne. Nous considérons la perte de la fonction "communication" comme une défaillance du système pour analyser les conséquences et chercher les comportements sûrs basés sur l'expertise du domaine. Evidemment, cette approche hérite des inconvénients de l'AMDE : longue, lourde, complexe et nécessitant une connaissance approfondie du système analysé.

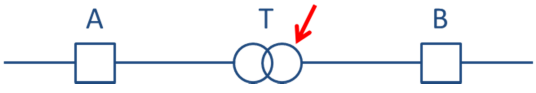

Figure 7. Portion de ligne électrique, exemple

Prenons un exemple fictif pour illustrer la démarche. Sur la portion de ligne de la figure 7, dans le cas d'un défaut de surintensité au niveau du transformateur T, supposons que le scenario de protection prévoit que le disjoncteur A s'ouvre puis le disjoncteur B. Un faux message GOOSE indiquant à B que A est bien ouvert alors que ce

n’est pas le cas correspond à une défaillance dont l’effet serait l’ouverture de B et l’apparition d’un arc électrique, ce qui doit être éviter. L’AMDE doit nous permettre d’identifier l’ensemble des défaillances aux conséquences indésirables pour implémenter les programmes alternatifs "mode de fonctionnement « sûr »".

Pour le cas particulier des SAS, nous nous inspirons d'une technique de temporisation dérivée des schémas de protection classiques.

3.2. La sélectivité électrique

Dans le domaine de la protection électrique, la sélectivité consiste à localiser et déconnecter la partie du réseau en défaut, et seulement celle-ci, en maintenant sous tension la plus grande partie possible de l’installation [Nereau 2001]. Il existe différentes méthodes pour assurer la sélectivité : la sélectivité ampèremétrique par les courants, chronométrique par le temps, logique par échanges d’information, par protection directionnelle, par protection différentielle [MG 2003]. Il est possible de combiner deux types de sélectivité pour exploiter leurs avantages de façon complémentaire, apportant par exemple redondance ou secours. Par exemple, il est possible d’associer une sélectivité chronométrique à une sélectivité logique pour palier un défaut d’attente logique.

Dans le cas d’une sélectivité chronométrique, le défaut représenté sur la figure 8 est vu par les protections A, B, C et D. C’est le disjoncteur en D qui déclenche le premier (0,2s après la détection du courant de défaut) puis si celui-ci est défaillant et ne s’est pas ouvert, la protection en C se déclenche après un temps plus long, etc… Les relais en amont ne déclenchent que si les précédents ont échoué à éliminer le courant de défaut. La sélectivité logique permet de réduire considérablement le temps d’élimination du défaut car il n’est plus nécessaire d’avoir une temporisation croissante quand on se rapproche de la source : c’est le relais le plus proche du défaut qui envoie un ordre d’attente empêchant les relais amont de déclencher. Un secours est en général ajouté à la sélectivité logique avec une sélectivité chronométrique en cas de défaut d’attente logique tel qu’un ordre d’attente permanent.

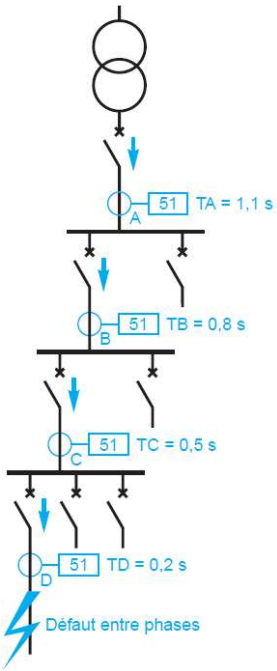

Figure 8. Principe de la sélectivité chronométrique [MG 2003]

Nous nous sommes inspirés de cette technique de protection électrique par sélectivité logique doublée d’un secours chronométrique pour proposer un mode de fonctionnement du SAS résilient aux "défauts" des communications GOOSE. Dans le cas normal (niveau de confiance des messages GOOSE élevé), un IED reçoit un message GOOSE et attend une éventuelle alerte de

cyber-incident du SCADA. Si après un temps t configuré, il n'y a pas eu d'alerte alors l'IED exécute le programme déclenché par le contenu du message. Par contre si l'IED reçoit une alerte, il va lancer un programme alternatif indépendant de la communication GOOSE et reste dans ce mode tant que l'alerte n'est pas levée. L'exemple suivant détaille cette technique qui permet d'assurer le temps de réaction de la sonde de détection des faux messages GOOSE.

4. Architecture de test

Le système électrique sur lequel nous menons notre étude est un couplage de deux jeux de barres. De part et d'autre du couplage, chacune des deux sections alimente plusieurs lignes de transformation par son propre générateur. En fonctionnement normal le couplage est ouvert. Dans le cas d'un défaut au niveau du générateur de la première section, celle-ci n'est plus alimentée. Il s'agit alors de faire automatiquement la commutation permettant au générateur de la deuxième section d'alimenter la section 1, en ouvrant le disjoncteur du générateur 1 afin d'isoler le défaut puis en fermant le couplage. Chacune des alimentations ainsi que le couplage sont gérés par leurs propres IED. L'architecture électrique représentée sur la figure 6 est simplifiée : les lignes de transformation n'apparaissent pas.

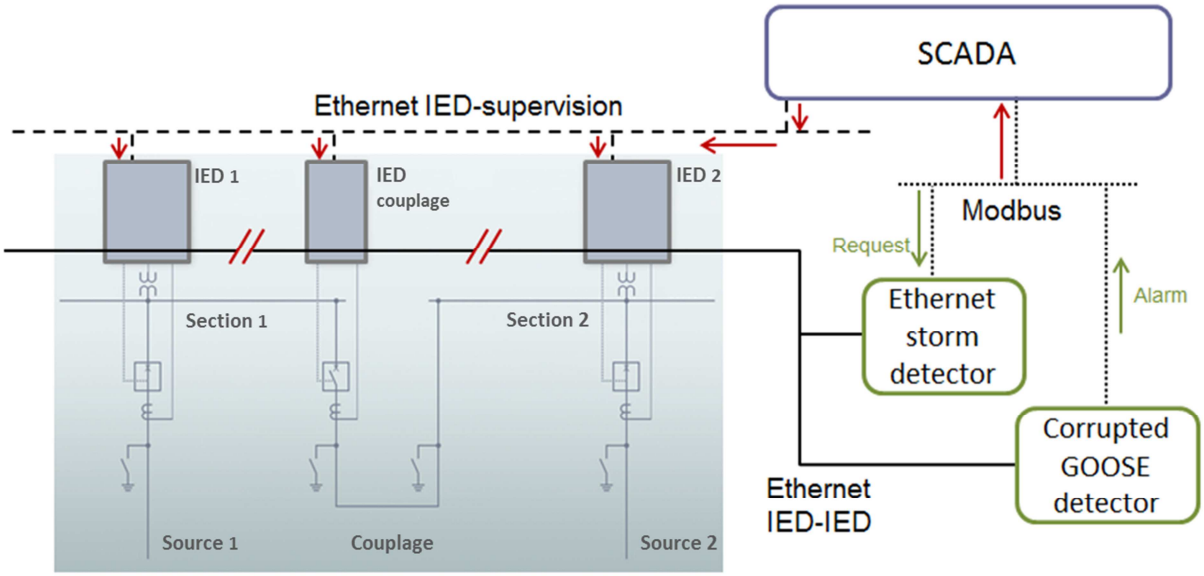

Figure 6. Architecture électrique et de communication

En fonctionnement normal, une temporisation force les IED à attendre jusqu'à l'expiration du temps maximal de détection de fausses trames GOOSE. Cela est envisageable car les grandeurs temporelles des fonctions de protection sont de l'ordre de 100ms voire 1s [MG 2003] alors que le temps de transfert total d'un message GOOSE doit être au maximum de 4ms.

Le mode sûr (obtenu par AMDE) est particulièrement simple dans ce cas. Il suffit de positionner le couplage en position ouverte et de ne pas générer le signal de fermeture des disjoncteurs. Le système revient en mode normal dès que le superviseur désactive l'alarme.

Les tests sur les performances du système en termes de temps de réaction et dégradation de la performance du réseau de distribution sont en cours.

V. Conclusions

Nous avons proposé une architecture intégrant les capteurs de cyber-incident dans le superviseur SCADA afin de permettre la détection des attaques sur les communications temps-réel dans les SAS 61850 et le fonctionnement du système dans un mode dégradé malgré les attaques au niveau temps-réel. Nous avons réalisé deux sondes simples dont une qui permet de répondre à la clause 6.10.2 (détection des faux messages GOOSE) du standard IEC 62351-1. Après l'évaluation des performances des sondes sur notre maquette de test (temps de détection des tempêtes et faux

messages GOOSE) ainsi que du temps de réaction du système d'alerte (passage en mode dégradé) nous envisageons d'améliorer le fonctionnement en mode dégradé en introduisant, par exemple, une propagation des informations d'état par le réseau de supervision en cas de cyber-incident, autrement dit d'utiliser la communication "verticale" pour assurer le transfert de l'information normalement réalisé par la communication "horizontale".

Références

[Cheung 2007] Cheung S., Dutertre B., Fong M., Lindqvist U., Skinner K., Valdes A. (2007), Using model-based intrusion detection for SCADA networks. SCADA Security, Proc. intern. scientific symp., Miami Beach, Florida, USA, 24-25 January 2007

[Dessiatnikoff 2012] Dessiatnikoff A., Deswarte Y., Alata E., Nicomette V. (2012),Potential Attacks on Onboard Aerospace Systems, Security & Privacy, IEEE 10(4): 71-74

[Fovino 2012] Nai Fovino I., Coletta A., Carcano A., Masera M. (2012), Critical state-based filtering system for securing SCADA network protocols, IEEE Transactions on Industrial Electronics 59(10): 3943-3950

[Hong 2014] Hong J., Liu C.-C., Govindarasu M. (2014). Integrated Anomaly Detection for Cyber Security of the Substations, IEEE Transactions on Smart Grid 5(4): 1643-1653

[Hoyos 2012] Hoyos J., Dehus M., Brown T. (2012), Exploiting the GOOSE protocol: A practical attack on cyber-infrastructure, IEEE Globecom Workshops

[IEC 2009] IEC 62351 Parts 1-8 - Power systems management and associated information exchange – Data and communications security. 2009

[IEC 2012] IEC 61850 Communication Networks and Systems for Power Utility Automation, 2012

[Kirsch 2014] Kirsch J., Goose S., Amir Y., Wei D., Skare P. (2014), Survivable SCADA via Intrusion-Tolerant Replication, IEEE Transactions on Smart Grid 5(1): 60-70

[Koopman 2013] Koopman P., Szilagyi C. (2013), Integrity in Embedded Control Networks, Security & Privacy, IEEE 11(3): 61-63

[Kriger 2013] Kriger C., Behardien S., Retonda-Modiya J. (2013), A Detailed Analysis of the GOOSE Message Structure in an IEC 61850 Standard-Based Substation Automation System, INT J COMPUT COMMUN 8(5):708-721

[MG 2003] Merlin Gerin, Protection des réseaux électriques – Guide de la protection, 2003.

[Nereau 2001] Nereau J.-P., Schneider Electric, Cahier technique n°201, Sélectivité avec les disjoncteurs de puissance basse tension, mars 2001

[NRC 2007] NRC, Effects of Ethernet-based, Non-safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations, NRC Information notice 2007-15

[Premaratne 2010] Premaratne U., Samarabandu J., Sidhu T., Beresh R., Tan J.-C. (2010), An intrusion detection system for IEC 61850 automated substations, IEEE Transactions on Power Delivery 25: 2376–2383.

[Siemens 2014] SIPROTEC 5 PIXIT, PICS, TICS IEC 61850 Manual v06.00, C53000-G5040-C013-4.00, 2014